USAWC STRATEGY RESEARCH PROJECT

"NO SILVER BULLET": MANAGING THE WAYS AND MEANS OF CONTAINER SECURITY

by

LTC Michael J. Babul
United States Army Reserve

Professor Dallas Owens
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **03 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **No Silver Bullet Managing the Ways and Means of Container Security**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Michael Babul**		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**29**	

ABSTRACT

AUTHOR: LTC Michael J. Babul

TITLE: “No Silver Bullet”: Managing the Ways and Means of Container Security

FORMAT: Strategy Research Project

DATE: 27 January 2004 PAGES: 29 CLASSIFICATION: Unclassified

The vulnerability of our seaports to acts of terrorism in which cargo containers are utilized to transport the means to cause damage to our infrastructure, our people, and our economy is significant. This project will address the reality of the threat. It will investigate the measures being undertaken or considered to address our vulnerabilities to the threat and will analyze the anticipated effects of these measures in comparison with estimated costs and the means available to the stakeholders sharing the financial responsibilities for their implementation. A basic assumption is that a fail-safe program to ensure container security is improbable and cost-prohibitive. Therefore, by managing risk, priorities will be established. Upon analysis of the findings of the research, this paper will recommend ways to best utilize the available means to maximize container security and minimize our US seaport vulnerability to acts of cargo container-borne terrorism.

TABLE OF CONTENTS

"NO SILVER BULLET": MANAGING THE WAYS AND MEANS OF CONTAINER SECURITY

The globalized economy of the 21st Century is dependent upon freely flowing trade that has been facilitated by increases in containerization of cargo and the use of multi-modal conveyances throughout the international shipping industry. The efficient use of cargo containers has transformed business processes that now rely heavily upon "just-in-time" deliveries and reduced inventories. Since the attacks on the World Trade Center, expeditious, uninterrupted movement of ocean-going cargo is no longer a certainty. The new reality is that our nation is vulnerable to terrorist attacks on its people, infrastructure, and economy.

Seaports are the "critical gateways"[1] for international commerce. More than ninety-five percent of our non-North American foreign trade passes through our seaports. More than five thousand vessels carrying cargoes from around the world transit our ports each year.[2] More than seven million containers enter the country annually.[3] Delay or interruption to this flow is economically intolerable. In addition, while our seaports vary in size and traffic, most are located in or near major metropolitan areas, where attacks would leave large populations vulnerable.[4] For these reasons targeting U.S. seaports provides terrorists with a way to inflict significant consequences on our economy, as well as our citizens. Currently, most security professionals agree that no "silver bullet" exists to solve the container security problem, so "we deploy our finite resources and manpower against the highest risks in hope of preventing the most catastrophic and deadly scenarios."[5]

HOW REAL IS THE THREAT?

Consider the following condensed scenario posed by Robert Williscroft. "A container ship is putting into the Port of Long Beach, the largest port on the West Coast. A Coast Guard cutter is standing off the starboard side, awaiting permission to board the vessel for a routine customs and security inspection. The check is routine, but the Coast Guard inspects only two percent of incoming containers, which means that only a small percentage of incoming vessels are actually boarded. To the north, a Bahamian-registered container ship has just entered Puget Sound. The Coast Guard waves this ship on. Protocol indicates that the next vessel will be boarded. Many miles to the east, a container ship makes its way to New York harbor. As in Seattle, the Coast Guard waves the ship on, since it had just boarded another vessel twenty minutes earlier.

Deep inside each vessel, in three containers well buried under dozens of other containers, three simple devices sense that all motion in the vessels has ceased. A set of timers starts. Fifteen minutes later, the sensors determine that the vessels still have not moved, and begin to

charge banks of capacitors from groups of lead-acid automobile batteries located nearby inside the containers. In a few seconds three igniters explode, ramming shaped blocks of plutonium against plutonium targets. In a heartbeat, nearly simultaneously in Long Beach, Seattle, and New York harbors, 10 kilotons of nuclear fire is unleashed dockside. For a thousand feet in all directions, everything is incinerated in a massive fireball. The blast front destroys everything but the most massive buildings for a mile beyond that. Hundreds of thousands die in less than a minute since the capacitor banks first discharged."[6]

While this portrayal represents a fictitious scenario that a terrorist organization might use to inflict devastating damage to our people, our infrastructure, and our economy; the following accounts represent the real facts as we weigh the likelihood of a possible terrorist attack on a major U.S. seaport via the maritime industry. In 2001 a suspected member of the Al Qaeda terrorist network was arrested in Italy after he tried to stow-away in a shipping container heading to Toronto. The container was furnished with a bed, a toilet, and its own power source to operate the heater and recharge batteries. According to the Toronto Sun, the man also had a global satellite telephone, a laptop computer, an airline mechanic's certificate, and security passes for airports in Canada, Thailand, and Egypt.[7] A March 2002 report by Norwegian intelligence has identified twenty-three merchant vessels believed to be linked to al Qaeda. Some of the vessels are thought to be owned outright by Osama bin Laden's business interests, while others are on long-term charter.[8] The Times of London reported that bin Laden used his ships to import into Kenya the explosives used to destroy the U.S. embassies in Kenya and Tanzania.[9] In October 2002, a French-flagged tanker was attacked by terrorists in a manner quite similar to the attack on the USS Cole in 2000. The attack resulted in 60,000 tons of oil being discharged into the waters off Yemen and killing one crew member.[10] In 2002 the FBI apprehended a U.S.-born Muslim convert suspected of being part of an al Qaeda cell attempting to set off a "dirty bomb" designed to scatter deadly radioactive material.[11] Just recently in Moldova, a former Soviet republic, dozens of rockets, whose warheads were outfitted with the so-called "dirty bombs," were reported to be missing from a depot near Trans-Dniester Tiraspol military airport.[12]

These accounts are factual. The terrorist threat to our seaports is real. Cargo containers provide terrorists with potential platforms that are numerous and unwieldy, as well as difficult and expensive to search. They present an easily accessible conveyance for a nuclear weapon or radiological "dirty bomb." As the result of inadequate security at points of origin and major seaports of embarkation and debarkation, our vulnerability to attack is significant. The U.S. government and private industry cannot afford to be complacent and must come to consensus

on appropriate security measures and standards. More importantly, the two must decide how, as mutual stakeholders, they will share the costs associated with the measures being considered for implementation.

THE ECONOMIC IMPACT OF A WMD ATTACK AT A SEAPORT

An April 2003 study conducted by Abt Associates, Inc. assumed the detonation of a 10-20 Kiloton cargo container-delivered fission weapon on a major seaport or Washington, DC. The costs and consequences of such an attack were astounding. In the three possible scenarios examined, it was estimated that the disruption created in U.S. trade would cost from $100-200 billion. Property damage estimates ranged from $50-500 billion. Indirect cost estimates reached a high of $1.4 trillion. These indirect costs would be the result of global, long-term effects caused by the responses to such a WMD attack. Indirect costs would include items such as increases in insurance premiums, devalued stock prices for affected companies, slowing or shutting down of production lines, and loss of confidence in the "just-in-time" delivery process. The loss of confidence in the "just-in-time" delivery process would result in manufacturers and wholesalers assuming increased inventory holdings to counter unpredictable trade flow. This increased inventory would cost an estimated $50-80 billion. While it is impossible to accurately place a dollar value on human life, the Abt study estimated that loss of life, which in Manhattan for instance could reach as high as one million deaths, would cost up to $3 trillion (30% of US GDP).[13]

In October 2002 Booz, Allen, Hamilton, a consulting firm, conducted a war game to test government and industry responses to the threat of a major terrorist attack involving both conventional and radiological bombs smuggled into the U.S. ports in multi-modal cargo containers. The war game involved the discovery of a radiological bomb in Los Angeles, the arrest of three men on the FBI watch list at the Port of Savannah, and the subsequent disclosure by one of the suspects apprehended in Savannah of a coordinated al Qaeda plot to target multiple U.S. seaports. Simulated actions taken and reactions anticipated during the war game included the immediate closure of the Ports of Los Angeles and Savannah, activation of the California National Guard, inspection of all trucks carrying containers in the U.S., closure of all U.S. ports, sharp decreases in stock values, and major increases in gas prices. The war game confirmed that reactions provoked by an attack or threat of attack result in indirect costs that dwarf the direct costs of such an incident.[14]

Various other experts have estimated the costs to our economy due to the discovery or detonation of a nuclear or radiological device at a seaport, subsequent port closures, or just

from general disruptions to the supply chain. In May 2002 the Brookings Institution published a report that estimated the costs associated with port closures from a WMD attack could reach $1 trillion.[15] In October 2002, in response to a labor dispute, all West Coast ports were closed for eleven days. This closure and the weeks of eliminating the backlog of cargo resulted in losses estimated in the billions of dollars.[16] A study by the Georgia Institute of Technology found that when a company announces a supply chain disruption, it can expect a drop in its stock price of almost nine percent.[17] Any disruption to the flow of free trade will have significant costs. However, the serious consequences of a WMD attack on a U.S. seaport would be devastating to our economy.

A MULTI-LAYERED APPROACH TO CONTAINER SECURITY

The U.S. government, in partnership with the international community and the private sector, has begun to address the container security issue in hopes of minimizing our vulnerabilities. Key points of vulnerability from origin to destination are readily identifiable and must be addressed. Overseas warehouses loading containers for export have weak controls and personnel usually lack detailed background checks. Seals attached to containers provide little additional security. Trucking companies offer little in-transit visibility for containers as they are shipped from warehouse to the ports of embarkation. At the terminals containers are at risk of tampering as they await upload aboard a container vessel. Security measures at terminals are often inadequate and the same personnel risks exist as are found at points of origin. Seals are seldom checked for signs of tampering prior to and during loading. Vessels may make multiple port calls before they reach their final destination and containers are subject to tampering at each stop along the route.[18]

While no “silver bullet” exists to provide a 100% secure cargo container environment, there appears to be consensus that the optimal approach involves a system of systems – a multi-layered approach that incorporates security measures at all links in the supply chain from manufacturer to consumer. The key tenets of a comprehensive container security strategy include: risk analysis, container integrity, container tracking and tracing, and container load verification.[19] Government regulation and incentives, multilateral and bilateral agreements, and voluntary measures taken by the private sector are now being implemented or considered to address the container security issue.

The Port and Maritime Security Act of 2001 evolved into the Maritime and Transportation Security Act (MTSA) of 2002. This legislation was signed by President Bush on 25 November 2002 and was designed to protect our nation’s seaports and waterways from terrorist attack.

The major components of the MTSA are: Threat and Security Assessments, Security Plans and Advisory Committees, and Grants. Other key features involve intelligence, personnel and cargo identification systems, extended seaward jurisdiction, and training. The Department of Homeland Security (DHS) has been charged with oversight of the MTSA. [20]

DHS has published a comprehensive strategy for port security that is based on: Enhancing our Nation's Security, Shielding our Maritime Borders and Ports, Managing the Threats, Coordinating our Response, and Providing Leadership. In implementing this strategy, DHS has undertaken a number of initiatives designed to further reduce port vulnerabilities.[21]

The Port Security Grant Program, managed by the Transportation Security Administration (TSA), funds security planning and projects to improve dockside and perimeter security. In FY03 170 million dollars was distributed to our key ports, with the bulk of those funds going to our 17 strategic seaports designated for the deployment and redeployment of military cargo. However, this represents only a fraction of what the American Association of Port Authorities considers necessary to address the myriad of security deficiencies at our U.S. seaports.[22]
The Container Security Initiative (CSI) is a DHS program that incorporates teamwork among domestic and foreign port authorities. The program is designed to identify, target, and search high-risk cargo at ports of embarkation. CSI consists of four core elements: (1) Establishing security criteria for identifying high-risk containers based on advance information. (2) Pre-screening containers at the earliest possible point. (3) Using technology to quickly pre-screen high-risk containers. (4) Developing secure and "smart" containers.[23] The program has expanded to 20 major ports around the world, which account for about 68% of our total container imports. Under the CSI program, the screening for weapons of mass destruction in cargo containers is accomplished by highly-skilled Customs and Border Protection (CBP) officials deployed to work in concert with their equally proficient host nation counterparts. This is considered an essential positive step in reducing our vulnerability to terrorist attack, as many would characterize inspections at the ports of debarkation as being too late. Sharing of intelligence and leveraging of technology are essential to the long term success of this initiative.[24]

Operation Safe Commerce (OSC) is a new partnership between the public and private sectors, whose aim is enhancing security throughout international and domestic supply chains while facilitating the efficient movement of legitimate, international commerce. OSC started as a New Hampshire-based, public-private partnership in which various "law enforcement entities and key private sector entities combined efforts to design, develop, and implement a means to test available technology and procedures in order to develop secure supply chains."[25] The

initiative analyzed a supply chain shipment between Europe and New England. The container shipment was equipped with onboard tracking sensors and door seals. It was continually monitored at the various transportation nodes as it passed through the supply chain. OSC is intended to validate security at the point of origin and demonstrate what is needed to ensure that parties associated with commercial shipping demonstrate care and diligence in packing, securing, and manifesting the contents of a shipment of goods in a container.[26] In addition, OSC will demonstrate various methods to ensure that the information and documentation associated with these shipments is complete, accurate, and secure from unauthorized access. The project will ultimately gauge the security of the supply chain with these new procedures in order to determine their viability.

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a plan which expands the security process throughout the supply chain. The plan provides incentives to private industry through preferential treatment during the shipping process. C-TPAT's intent is to increase cargo security while improving the flow of trade. Seven of America's Fortune 500 companies helped Customs develop the program. More than eighty companies initially signed C-TPAT agreements with the Customs Service. More than 4000 companies are expected to participate in this voluntary program by 2004. Under C-TPAT, businesses will implement comprehensive self-assessment procedures for their supply chain using the security guidelines developed in conjunction with the Customs Service. In addition, they must familiarize companies in their supply chain with the guidelines and the program. The goal is for these businesses to provide Customs with detailed and relevant information about their trucks, drivers, cargo, suppliers, and routes. As C-TPAT members, companies would become eligible for expedited processing and reduced inspections.[27]

The U.N.'s International Maritime Organization created the International Ship and Port Facility Security Code (ISPS), which has been adopted by a majority of countries. The ISPS Code is the first multilateral ship and port security standard and is scheduled to be implemented in 2004. In essence, the Code takes the approach that ensuring the security of ships and port facilities is basically a risk management activity and that to determine what security measures are appropriate, an assessment of the risks must be made in each particular case. Port and vessel operators would be responsible for conducting the necessary assessments, developing and implementing security plans, hiring security officers, and conducting appropriate training.[28] Smart and Secure Tradelanes (SST) is a supply chain security program funded by private industry. The SST initiative was founded on the premise that considerable gaps in international supply chain security exist and endanger continued prosperity, freely flowing trade, and

economic development. The SST industry consortium has studied potential ways it might provide economic incentives to finding, innovating, and implementing efficient and effective security solutions. During the past year, the Smart and Secure Tradelanes initiative became the largest cargo security program in operation, assisting international shippers in automatically tracking the location and status of containers while creating a system to detect and report container tampering. The second phase of SST will focus on expanding the global network, extending operations, and integrating into existing supply chain systems new technologies such as "smart" containers, equipped with electronic seals and multiple sensors.[29]

The 24-Hour Advanced Manifest Rule requires every ship bound for a U.S. port to provide a detailed cargo listing 24 hours prior to loading. This rule became effective in December 2002, but was not fully enforced until February 2003. The rule is intended to provide time to perform a risk analysis of an inbound container. Failure to comply with the rule results in cargo not being loaded and could result in additional penalties to the shipper. The rule is another way the U.S. is trying to extend its defensive perimeter to the ports of embarkation.[30]

The 96-Hour Advance Notification of Arrival Rule requires submission of detailed crew, cargo, vessel history, and passenger information to DHS's new National Vessel Movement Center. This deadline enables advance boarding of suspect vessels well before they reach our shores. Ship operators have shown little objection to this rule, however they have expressed concern with enforcement of the manifesting of crew members due to the difficulty in performing required background checks. New biometric technologies are being developed to assist in this effort.[31]

LEVERAGING NEW AND EXISTING TECHNOLOGIES

Fixed drive-through, crane mounted, and mobile screening systems are now available to detect radiological emissions. These sensitive radiation monitoring systems utilizing glass fiber sensors are capable of detecting nuclear materials in shipping containers. New gamma ray technologies are being developed by companies such as Science Applications International Corporation (SAIC). Gamma ray sources provide a safer and more cost-effective solution to cargo screening than traditional x-ray systems. These new systems have a throughput of up to ten times greater than x-ray systems. Gamma ray detection devices allow for minimal delay in movement of cargo, with cycle times less than a minute per container, and they offer the possibility of 100% screening of cargo at foreign ports.[32]

The Savi Transportation Security System is a web-based application that offers continuous online cargo tracking, security monitoring, and management of containers and their

contents. It provides an automatic, electronic audit trail that enables a container and contents to be verified and fast-tracked through an inspection. It enables users to consistently monitor container integrity, verifies that a container was loaded at a secure site according to approved procedures, and it gathers data to conduct a virtual inspection prior to arrival.[33]

DHS is developing the ACE Project (Automated Commercial Environment). ACE is the initial modernization project that will expedite trade across U.S. borders while providing the tools, information, and foresight needed to target suspect trade shipments faster and more accurately. This $1.7 billion endeavor will provide CBP with a multi-agency information sharing and targeting system.[34] It will link a variety of databases to include those of shippers, freight forwarders, importers and exporters with DHS, TSA, CBP, and various law enforcement and intelligence agencies.

The shipping industry is investigating the production of a "smart container." This container would have technological systems and sensors in place to monitor its contents, integrity, and location. Radio Frequency Identification Devices (RFID) would be affixed to each container and would transmit a signal that would be incorporated with a GPS system to provide continuous status of its location. Electronic seals would be connected to the devices to monitor the integrity of the container. In addition, the technology exists to seal each container with a metallic flake caulk that emits a unique magnetic signature. Using a hand-held device the magnetic signature can be read into an encrypted database. The container can then be scanned electronically at each handling as it transits from origin to destination. Breeching of the container would alter the magnetic signature and preclude a container with an altered magnetic signature from entry into the port of debarkation until physically inspected.[35] Low-cost sensors are available to monitor for explosives or other hazardous chemicals. Currently the industry has not yet agreed upon a standard for the "smart container" with added cost being another consideration.

THE COSTS OF IMPROVED CONTAINER SECURITY

The federal funding provided thus far represents only a small portion of the anticipated costs for improvements recommended by the Interagency Commission on Crime and Security of U.S. Seaports. Grant applications far exceed the available resources. The USCG has estimated port security requirements will cost about $4.4 billion over ten years.[36] Heightened national security alert levels require ports to assume additional costs beyond that figure, as well. U.S. seaports estimate that it will take $2.2 billion to address immediate needs to meet proposed requirements.[37] If we were to extend the requirements to every U.S. manufacturer, wholesaler, retailer, shipper, and warehouse establishment and assume that each invested fifty

thousand dollars in personnel and technological security improvements, the cumulative bill would exceed $83 billion.[38]

Arguably money is more effectively spent ensuring that a weapon of mass destruction never finds its way into a cargo container bound for the United States. To meet this end additional manpower and technologies must be applied at the point of origin in the manufacturers' warehouses and at the ports of embarkation. Forward deployment of personnel and screening technologies are feasible and will facilitate 100% inspection or screening of cargo containers bound for U.S. seaports.

Approximately 19,000 containers per day are loaded in foreign countries for shipment to the United States. Assuming that an inspector can supervise the loading of eight to ten containers per day, it would take 1900-2300 inspectors working an 8-10 hour day over seven days to oversee the workload. Realistically the total number would be closer to 4000 based on a normal work week schedule and administrative overhead. At an estimated $50,000 per year salary per inspector, the projected cost for such an inspection program would be $2 billion annually – money well spent at what many consider the most crucial point of the supply chain.[39]

The Abt study estimated that it would cost $100 million annually to employ the screening technologies available to ensure 100% screening of cargo transiting a major port. At this rate it would require $10 billion to establish 100% screening capability at one hundred major international ports.[40] Various screening systems average about $1.2 million per unit and can process about fifteen containers per hour.[41] Lesser ports would require a corresponding number of screening systems as related to the total volume of container traffic destined for the United States.

The ISPS Code mandates international shippers and ports meet specific security standards which include Automated Identification Systems, Company and Port Security Officers, Vessel and Port Security Assessments and Plans, training, and equipment. It is estimated that implementation of these standards would cost an initial $1.3 billion and $730 million annually thereafter.[42]

It is too early to gauge the costs of implementation of MTSA, CSI, C-TPAT, and the 24-hour and 96-hour rules. Initial estimates of the cost of the 24-hour rule vary greatly from 281 million to $10 billion per year.[43] The FY04 proposed budget for CSI was $61 million[44] and the proposed budget for C-TPAT was $12.1 million.[45] As previously stated, the ACE project will cost an estimated $1.7 billion to provide the CBP with the linkages to various databases required to address our vulnerabilities.

END STATE: THE LAYERED STRATEGY COMES TOGETHER

DHS considers the following scenario as a desirable end state for a comprehensive, container security program. A container of auto parts is scheduled for shipment from a manufacturer in China to a large supplier in California. The manufacturer and shipping company are members of C-TPAT and have voluntarily taken steps to prevent unauthorized access to the container. They have increased lighting at their facilities, improved fencing, and added video surveillance. The shipper is using a "smart container," utilizing the latest technology and recommended by OSC. The shipper transmits the manifest information according to the 24-hour rule. CBP analyzes the data and compares it against an Automated Targeting System. CBP officers stationed at the port as part of CSI review the results and with host nation counterparts approve the container for shipment.

The container is loaded upon the vessel and once underway CBP transmits the manifest to the USCG and TSA. Prior to 96 hours before entering the U.S. the vessel operator sends a vessel and crew identification message to the USCG. The USCG performs a threat analysis based on received data. If flagged, the vessel is boarded by a team of trained CBP officers, Sea Marshals, and USCG. Once cleared the vessel continues to the port.

At the port CBP ensures that only manifested containers are discharged. Video surveillance equipment purchased with TSA grant money monitors the container staging areas. Upon closer inspection, it is noted that the container seal is scratched and that the container had been in a vulnerable area aboard the vessel. The container is then designated for a non-intrusive gamma ray screening. The results of the screening appear to match the manifest and the container is released for shipment to the importer and arrives at its final destination with cargo intact.

WHO WILL PAY FOR CONTAINER SECURITY?

While the stakeholders agree on the multi-layered, risk managed end-state for container security as depicted above, there is major disagreement on how much of the burden each stakeholder should assume. The estimated cost is substantial, but the cost of inaction might prove to be tremendous. However, each of the major stakeholders is likely to reap significant benefits from the recommended or mandated improvements. Tighter security measures could result in the government obtaining more than $2 billion in additional tariffs from identification of cargo that had previously been fraudulently misidentified or unidentified.[46] Furthermore, it is estimated that governments would realize over $16 billion in additional tobacco tax revenues alone through these improvements.[47] Increased security would have an impact on reducing

illegal drug trafficking and illegal immigration. The manufacturing and shipping industries would experience sizable gains through decreased theft and pilferage. The Federal Bureau of Investigation estimates the cost of container cargo losses between $10-12 billion per year.[48] In addition, industry would benefit from lowered insurance premiums, reduced delays, faster processing times, improved inventory control, and decreased payroll through leveraging information technology. These gains may, in fact, outweigh the costs of the security improvements being mandated or considered. The Strategic Council on Security Technology (SCST), an independent industry group of shipping companies, port operators, and Information Technology vendors conducted a test using web-based software, RFID tags, electronic seals, and other technologies. Over sixty companies shipped more than eight hundred containers across three continents and realized savings that ranged from $378-462 per container. With more than 7 million containers entering U.S. seaports in 2002, the cumulative savings would be approximately $3 billion.[49]

Deciding how to pay for planned security improvements is a challenge. Given the importance of our seaports to our economic infrastructure, it has been argued by the American Association of Port Authorities (AAPA) that additional fees and taxes upon the ports are unacceptable. There already exist 124 different user fees and taxes, which contribute to a combined $22 billion of federal revenues generated by the ports annually.[50] The AAPA advocates the federal government assume the major portion of the increased security costs.

In October 2003, Thomas Thune Andersen, CEO of Maersk Inc., speaking at the 2nd Annual U.S. Maritime Security Expo and Conference spoke to the cooperation needed to address maritime security issues. Mr. Anderson stated, “Security requirements are constantly changing and evolving. Progress has been made, but much work still lies ahead. No single entity can do it alone – everyone must work together. True government and industry partnerships are critical to success. We continue to work with government, industry, and customer groups to identify and refine measures that will be effective, sensible, and affordable.”[51]

When Homeland Security Secretary Tom Ridge visited the Port of Wilmington, DE in October 2003 to launch new maritime security guidelines published by the government, he addressed the question of who is to pay for improved security. Ridge indicated his department needed to "look more aggressively" at businesses that use ports, including terminal operators, vessel owners, and waterside facilities such as refineries and power plants. "Now is the time for us to have that very important public discussion with regard to the balance between public and private dollars to pay for security around private-sector assets," Ridge said.

Michael Connors, of Booz, Allen, Hamilton, also speaking at the 2nd Annual U.S. Maritime Security Expo and Conference, concluded that with the federal government running record deficits, nothing is on the horizon for other than seed money for technology development. He urged a public education effort to explain increased costs to consumers, because one way or the other they will be paying for it.

MILITARY BENEFITS

During a large scale deployment, the Department of Defense normally transports about 95 percent of all military equipment and supplies through 17 designated strategic seaports in the continental United States.[52] The Maritime and Transportation Security Act of 2002 and the International Ship and Port Facility Security Code mandate the conduct of vulnerability assessments, as well as the development of security plans for port facilities and vessels. These measures will result in a more secure environment for military equipment and supplies as they transit commercial seaports and are loaded aboard commercial cargo vessels. The initial 92 million dollars disbursed in TSA port security grants in 2002 went towards improving physical security at these strategic seaports. Improvements in fencing, lighting, sharing of information, and training of personnel were targeted as part of this TSA grant program. These physical security enhancements will reduce the vulnerability of military cargo to the same threats commercial cargo is subject to, as mentioned previously.

In addition, the requirement for military security personnel would be reduced as the result of mandated port security measures for commercial facilities. Military Surface Deployment and Distribution Command, formerly Military Traffic Management Command, has three wartraced, Reserve Component (RC) Port Security Companies. Two of these companies are aligned with ammunition ports on the east and west coast of the United States. The remaining company is incapable of providing security at all the other designated strategic seaports being utilized. During the most recent deployments for Operation Iraqi Freedom, non-Military Police RC units were mobilized to conduct the port security missions. The multi-layered initiatives being implemented to address container and seaport security would reduce the requirement to mobilize such units, thereby enabling Forces Command to better utilize their capabilities to support the Combatant Commanders.

Furthermore, technological developments in “smart containers” would offer the military great utility as it strives to improve In-Transit and Total Asset Visibility, as well as provide a more secure container. Improvements in automated cargo documentation and tracking systems

have potential military benefit as they would enhance the distribution process and provide better support to the warfighter.

RECOMMENDATIONS

The stakeholders must continue to work together to address the variety of issues related to improving maritime security and reducing our vulnerability to a terrorist attack utilizing a cargo container. The multi-layered measures developed thus far to ensure adequate levels of security at all nodes of the supply chain need to be fully funded and implemented. These mandated and recommended systems of solutions may not be as cost-prohibitive as many believe. Residual benefits, such as increased tax revenues, lower insurance premiums, and cargo loss prevention resulting from security improvements, will fund much of the added cost and government and industry must reach an accord as to how best fund what remains.

The strategy of extending our defensive perimeter to the foreign cities and ports where our container imports originate is the right strategy. The federal government should continue to work multilaterally and bilaterally within the international trade community to ensure that the necessary systems are in place to protect the citizens of the U.S., our infrastructure, and our economy.

Currently CBP is providing technical assistance to those countries that are not financially capable of implementing security measures to a level that would guarantee the safety of U.S. interests. We cannot afford the risk of allowing non-compliant countries to continue their trade with U.S. companies. Our federal government has two options with these non-compliant countries. Either we restrict trade with them or subsidize their efforts to comply with international and U.S. standards. It is in our best interest, however, to promote free trade with these lesser nations and not hinder their development. Therefore, our government should subsidize the development of improved screening technologies and the acquisition of necessary systems in sufficient quantities to those nations lacking adequate means to do so. In addition, we should expand CSI to provide trained inspection personnel at all international seaports with commerce links to the United States.

The private sector should assume the major portion of the cost for meeting improved security standards from point of origin in the supply chain and through movement to the ports of embarkation. Manufacturers, freight consolidators, freight forwarders, and shippers should invest in providing adequate personnel to oversee the stuffing of containers on their loading docks. Government should continue to provide incentives for companies to do so. Physical security costs in this link should also be assumed by the private sector. Manufacturers must

invest in “smart containers” and improved cargo tracking systems. The residual benefits realized from these security improvements would be significant and would offset a major portion of the cost of implementation. Those costs not offset should ultimately be passed on to the customer.

The federal government should continue to subsidize physical security and training at our U.S. ports through continued grants. The USCG is assigned the mission of providing adequate waterside security for our domestic ports. Within the new domestic security environment Congress should consider increasing USCG end-strength and providing the appropriate funding to accomplish the expanded mission.

State and local governments reap the benefits of additional tax revenues generated from well-operated ports. Therefore, state and local governments are stakeholders, as well, and should assume a portion of the costs of improving landside security at our domestic ports. These ports, whether they be state or privately operated, should also invest in providing high-tech screening systems, as significant security enhancements would likely attract additional cargo traffic, thus resulting in additional profits to offset the initial security investments.

EPILOGUE

DHS has no “silver bullet” to assist with its monumental assignment. The formidable tasks of coordinating and working with the many involved agencies to provide the required security to our nation’s seaports will not easily be accomplished. The MTSA, CSI, C-TPAT, SST, and OSC are significant steps in the right direction to help the U.S. reduce the vulnerability of its seaports to terrorist attack from water-borne cargo containers. While these represent potential ways, the necessary means to accomplish the desired end have yet to be fully identified. Debate over responsibilities in assuming costs is on-going, as “just-in-time” industry standards, finite resource allocations to DHS, and limited resources available to the ports hinder the total implementation of all measures required to ensure maximum security. Currently we have a “managed-risk, means-based” strategy, addressing areas of concern on a priority basis. The above recommendations provide a framework for addressing responsibilities. The American public can only hope it will not take a direct attack on a U.S. seaport to provide the impetus for the federal government and industry, as well as the other stakeholders, to determine the appropriate level of funding that each must provide to secure this vital component of our economic infrastructure.

WORD COUNT=5,959

ENDNOTES

[1] General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful.* (Washington, DC: U.S. General Accounting Office, August 2002), 3.

[2] Ibid.

[3] General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors.* (Washington, DC: U.S. General Accounting Office, July 2003), 1.

[4] General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful.* (Washington, DC: U.S. General Accounting Office, August 2002), 2.

[5] U.S. Department of Homeland Security, "Remarks by Secretary Tom Ridge at the Custom and Border Protection Trade Symposium," 20 November 2003; available from <http://www.dhs.gov/dhspublic/display?content=2324>; Internet; accessed 25 November 2003.

[6] Robert G. Williscroft, "A Solution for the Shipping Container Threat," 12 February 2003, available from <http://www.sftt.org/dwa/2003/2/12/2.html>; Internet; accessed 23 November 2003.

[7] Ernest Hollings, "Statement of Senator Ernest F. Hollings at the Senate Commerce Committee Field Hearing on Seaport Security," 19 February 2002; available from <http://hollings.senate.gov/~hollings/statements/2002709702.html>; Internet; accessed 23 November 2003.

[8] Joshua Sinai, "An Overview and Future Trends in Worldwide Maritime Terrorism," 7.

[9] Ernest Hollings, "Statement of Senator Ernest F. Hollings on Final Passage of S. 1214, the Maritime Transportation Security Act," 14 November 2002; available from <http://www.hollings.senate.gov/~hollings/ statements/2002B14648.html>; Internet; accessed 19 November 2003.

[10] Ibid.

[11] Donna Leinwand and Jack Kelley, "U.S. Citizen Arrested in 'Dirty Bomb' Plot," USA Today, 11 June 2002; available from <http://www.usatoday.com/news/nation/2002/06/10/terror-arrest.htm>; Internet; accessed 3 December 2003.

[12] Associated Press, "Rockets Said to Be Missing in Moldova," Los Angeles Times, 9 December 2003; available from <http://ebird.afis.osd.mil/cgi-bin/ebird/displaydata.pl?Requested=ebfiles/e20031209239809.html>; Internet; accessed 9 December 2003.

[13] Clark C. Abt, "The Economic Impact of Nuclear Terrorist Attacks on Freight Systems in an Age of Seaport Vulnerability," (Cambridge, MA, 2003), 3-5.

[14] Philippe Crist, “Security in Maritime Transport: Risk Factors and Economic Impact,” (Paris, Organization for Economic cooperation and Development, July 2003), available from <www.oecd.org/dataoecd/63/13/4375896.pdf>; Internet, accessed 15 November 2003.

[15] General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful.* (Washington, DC: U.S. General Accounting Office, August 2002), 4.

[16] Crist, 19-20.

[17] Dan Ross, “Supply Chain Link to the Bottom Line Debunking 5 Myths,” Optiant News, April 2002; available from <http://www.optiant.com/news_articles_fivemyths.html>; Internet, accessed 2 December 2003.

[18] General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors.* (Washington, DC: U.S. General Accounting Office, July 2003), 7.

[19] Maarten van de Voort and Kevin A. O’Brien, “Seacurity: Improving the Security of the Global Sea-Container Shipping System,” (Santa Monica, CA, Rand, 2003); 8.

[20] Department of Homeland Security, “Protecting America’s Ports,” (Washington, DC, 12 June 2003), 18; available from <www.dhs.gov/interweb/assetlibrary/Port_Security_Press_Kit_DHS.pdf>; Internet; accessed 10 November 2003.

[21] Ibid., 15.

[22] Ibid., 4.

[23] U.S. Department of State, “Fact Sheet: U.S. Customs Service’s Container Security Initiative,” 22 February 2002; available from <http://usinfo.state.gov/topical/pol/terror/02022505.htm>; Internet; accessed 27 September 2003.

[24] Ibid.

[25] Transportation Security Administration, “Operation Safe Commerce,” available from <http://www.tsa.gov/public/interapp/asset_summary_0122.xml>; Internet; accessed 9 October 2003.

[26] Ibid.

[27] Department of Customs and Border Protection, “*U.S. Customs Today: C-TPAT: Life in the FAST Lane,”* May 2002; available from <http://www.cbp.gov/xp/CustomsToday/2002/May/ctpat.xml>; Internet; accessed 27 September 2003.

[28] Department of Homeland Security, “Protecting America’s Ports,” (Washington, DC, 12 June 2003), 16; available from

<www.dhs.gov/interweb/assetlibrary/Port_Security_Press_Kit_DHS.pdf>; Internet; accessed 10 November 2003.

[29] Strategic Council on Security Technology, "Strategic Council on Security Technology Announces Second Phase of Smart and Secure Tradelanes Initiative," 12 November 2003; available from <http://www.scst.info/releases/nov12_03.html>; Internet; accessed 5 December 2003.

[30] Department of Homeland Security, "Protecting America's Ports," (Washington, DC, 12 June 2003), 17; available from <www.dhs.gov/interweb/assetlibrary/Port_Security_Press_Kit_DHS.pdf>; Internet; accessed 10 November 2003.

[31] Crist, 47.

[32] Michael P. Snell, "Gamma Ray Technology: The Practical Container Inspection Alternative," *Port Technology International*, n.d.

[33] Savi Technology Inc., Savi Transportation Security System. n.d.

[34] General Accounting Office, *Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions.* (Washington, DC: U.S. General Accounting Office, June 2003), 9.

[35] Williscroft, 3.

[36] American Association of Port Authorities, "Seaport Security," n.d.; available from <http://www.aapa-ports.org/govrelations/aapa_security_position.pdf>; Internet; accessed 27 September 2003.

[37] Richard Steinke, "Testimony before the Subcommittee on Coast Guard and Maritime Transportation – House Transportation and Infrastructure Committee," 14 March 2002; available from < http://www.house.gov/transportation/cgmt/03-14-02/steinke.html>; Internet; accessed 10 November 2003.

[38] Arc Advisory Group, *Trade Security: A Wildcard in Supply Chain Management.* (Dedham, MA: Arc Advisory Group, September 2002), 15.

[39] Williscroft, 3.

[40] Abt, 5.

[41] "A Closer Eye on Cargo," Christian Science Monitor, 14 August 2002; available from <http://www.csmonitor.com/2002/0814/p08s01-comv.htm>; Internet; accessed 27 November 2003.

[42] Crist, 4.

[43] Ibid., 49-52.

[44] General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors.* (Washington, DC: U.S. General Accounting Office, July 2003), 13.

[45] Ibid., 17.

[46] Michael Conners, principal Booz, Allen, Hamilton, speech at the 2nd Annual U.S. Maritime Security Expo attended by author, 29 October 2003, New York, NY.

[47] Peter J. Scrobe, VP and Manager AIMA Loss Control Services, presentation at the 2nd Annual U.S. Maritime Security Expo attended by author, 30 October 2003, New York, NY.

[48] Ibid.

[49] Dan Verton, "Shippers Face Big IT Security Costs but See Future Savings," 3 November 2003; available from <http://www.computerworld.com/printthis/2003/0,4814,8660,00.hm>; Internet; accessed 27 November 2003.

[50] Peter Zalewski, "Fees Would Hit Cruise Lines, Ocean Cargo," September 2002; available from http://southflorida.bizjournals.com/southflorida/stories/2002/09/02/story2.html>; Internet; accessed 27 November 2003.

[51] Thomas Andersen, President and CEO Maersk Inc., speech at the 2nd Annual U.S. Maritime Security Expo attended by author, 29 October 2003, New York, NY.

[52] General Accounting Office, *Combating Terrorism: Actions Needed to Improve Force Protection for DoD Deployments through Domestic Seaports.* (Washington, DC: U.S. General Accounting Office, October 200s), 1.

GLOSSARY

AAPA	American Association of Port Authorities
ACE	Automated Commercial Environment
CBP	Bureau of Customs and Border Patrol
CEO	Chief Executive Officer
CSI	Container Security Initiative
C-TPAT	Customs -Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOT	Department of Transportation
FY	Fiscal Year
GDP	Gross Domestic Product
GPS	Global Positioning System
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security Code
MTSA	Maritime Transportation Security Act
OSC	Operation Safe Commerce
RFID	Radio Frequency Identification Device
SAIC	Science Applications International Corporation
SCST	Strategic Council on Security Technology
SST	Smart and Secure Tradelanes
TSA	Transportation Security Administration
U.N.	United Nations
USCG	U.S. Coast Guard
WMD	Weapons of Mass Destruction

BIBLIOGRAPHY

Abt, Clark. The Economic Impact of Nuclear Terrorist Attacks on Freight Systems in an *Age of Seaport Vulnerability.* Cambridge, MA, April 30, 2003.

"A Closer Eye on Cargo," *Christian Science Monitor,* 14 August 2002. Available from <http://www.csmonitor.com/2002/0814/p08s01-comv.htm>. Internet. Accessed 27 November 2003.

American Association of Port Authorities. "Seaport Security," Available from<http://www.aapa-ports.org/govrelations/aapa_security_position.pdf>. Internet. Accessed 27 September 2003.

Andersen Thomas. Speech at the 2nd Annual U.S. Maritime Security Expo, New York, NY, 29 October 2003.

Arc Advisory Group, *Trade Security: A Wildcard in Supply Chain Management.* Dedham, MA: Arc Advisory Group, September 2002, 15.

Associated Press. "Rockets Said To Be Missing in Moldova," *Los Angeles Times,* 9December 2003. Available from <http://www.ebird.afis.osd.mil/cgi-bin/ebird/displaydata.pl?Requested=ebfiles/e20031209239809.html>. Internet. Accessed 9 December 2003.

Conners, Michael. Speech at the 2nd Annual U.S. Maritime Security Expo, New York, NY, 29 October 2003.

Crist, Phillipe. "Security in Maritime Transport: Risk Factor and Economic Impact," *Organization for Economic Cooperation and Development,* July 2003. Available from <http://www.oecd.org/dataoecd/63/13/4375896.pdf>. Internet. Accessed 15 November 2003.

Hollings, Ernest. *Statement of Senator Ernest Hollings at the Senate Commerce Committee Field Office Hearing on Seaport Security,* 19 February 2002. Available from <http://www.hollings.senate.gov/~hollings/statements/2002709702.html>. Internet. Accessed 23 November 2003.

Leiberman, Joseph. *Address to Government Affairs Committee,* 6 Dec 2002. Available from <http://www.senate.gov/~lieberman/press/01/12/2001C06B35.html>. Internet. Accessed 23 September 2003.

Leinwand, Donna and Jack Kelley. "U.S. Citizen Arrested in 'Dirty Bomb' Plot," *USAToday,* 11 June 2002. Available from <http://www.usatoday.com/news/nation/200206/10/terror-arrest.htm>. Internet. Accessed 3 December 2003.

Ross, Dan. "Supply Chain Link to the Bottom Line Debunking 5 Myths," *Optiant News,* April 2002. Available from <http://www.optiant.com/news_articles_fivemyths.html>. Internet. Accessed 2 December 2003.

Sanai, Joshua. *An Overview and Future Trends in Worldwide Maritime Terrorism.* Handout received at the 2nd Annual U.S. Maritime Security Expo, New York, NY, 29 October 2003.

Savi Technology Inc.. *Savi Transportation Security System* , Handout received at the 2nd Annual U.S. Maritime Security Expo, New York, NY, 29 October 2003.

Scrobe, Peter J. Presentation at the 2 nd Annual U.S. Maritime Security Expo, 30 October 2003, New York, NY.

Snell, Michael. "Gamma Ray Technology: The Practical Container Inspection Alternative," Port Technology International. n.d.

Steinke, Richard. "Testimony Before the Subcommittee on Coast Guard and Maritime

Transportation – House Transportation and Infrastructure Committee," 14 March 2002. Available from <http://www.house.gov/transportation/cgmt/03-14-02/steinke.html>. Internet. Accessed 10 November 2003.

Strategic Council on Security Technology. "Strategic Council on Security Technology Announces Second Phase of Smart and Secure Tradelanes Initiative," 12 November 2003. Available from http://www.scst.info/releases/nov12_03.html>. Internet. Accessed 5 December 2003.

Transportation Security Administration, *Operation Safe Commerce,* Available from <http://www.tsa.gov/public/interapp/asset_summary/asset_summary_0122.xml>. Internet. Accessed 9 October 2003.

U.S. Bureau of Customs and Border Protection, *CSI in Brief, January 2002,* Available from <http://customs.ustreas.gov/xp/cgov/import/cargo_ control/csi_in_brief.xml>. Internet. Accessed 9 October 2003.

U.S. Bureau of Customs and Border Protection, *U.S. Customs Today: C-TPAT: Life in The FAST Lane,* May 2002, Available from <http://www.cbp.gov/xp/CustomsToday/2002/May/ctpat.xml>. Internet. Accessed 9 October 2003.

U.S. Department of Homeland Security, *Implementation of MTSA Fact Sheet,* Washington, DC, July 2003. Available from <http://www.apaninfo.net/maritime/uploaded/docs /implementation%20of%20the%20MTSA.doc>. Internet. Accessed 10 November 2003.

U.S. Department of Homeland Security, *Press Release: Secretary Ridge Announces New* Initiatives *for Port Security,* 12 June 2003. Available from <http://www. dhs.gov/dhspublic/display?content=957>. Internet. Accessed 10 November 2003.

U.S. Department of Homeland Security, *Port Security: A Comprehensive Approach,* Washington, DC, June 2003. Available from <http://www.aapaorg/govrelations/port_security_fact_sheet.pdf>. Internet. Accessed 10 November 2003.

U.S. Department of Homeland Security, *Protecting America's Ports,* Washington, DC, June 12, 2003. Available from <http://www.dhs.gov/interweb/assetlibrary/Port_Security_Press_Kit_DHS.pdf>. Internet. Accessed 10 November 2003.

U.S. Department of State, Fact Sheet: U.S. Customs Service's Container Security Initiative, 22 February 2002. Available from <http://usinfo.state.gov/topical/pol/terror/02022505.htm>. Internet. Accessed 27 September 2003.

U.S. General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful.* Washington, DC: U.S. General Accounting Office, August 2002.

U.S. General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors.* Washington, DC: U.S. General Accounting Office, July 2003.

U.S. General Accounting Office, *Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions.* Washington, DC: U.S. General Accounting Office, June 2003.

Van de Voort, Maarten and Kevin O'Brien. " Seacurity: Improving the Security of the Global Sea-Container Shipping System," Santa Monica, CA, Rand, 2003.

Verton, Dan. "Shippers Face Big IT Security Costs But See Future Savings," 3 November 2003. Available from <http://www.computerworld.com/printthis/2003/0,4814,8660,00.hm>. Internet. Accessed 27 November 2003.

Williscroft, Robert. "A Solution for the Shipping Container Threat," 12 February 2003. Available from <http://www.sftt.or/dwa/2003/2/12/2.html>. Internet. Accessed 23 November 2003.

Zalewski, Peter. "Fees Would Hit Cruise Lines, Ocean Cargo," September 2002. Available from <http://southflorida.bizjournals.com/southflorida/stories/2002/09/02/story2.html>. Internet. Accessed 27 November 2003.